EXHIBIT 4

Freedom to Tinker

… is your freedom to understand, discuss, repair, and modify the technological devices you own.

« Does Sony's Copy Protection Infringe Copyrights?
What Does MediaMax Accomplish? »

More Suits Filed; MediaMax Insecurity Remains

Tuesday November 22, 2005 by Ed Felten

Yesterday two lawsuits were filed against Sony, by the Texas Attorney General and the EFF. The Texas suit claims that Sony's XCP technology violates the state's spyware law. The EFF suit claims that two Sony technologies, XCP and MediaMax, both violate various state laws.

One interesting aspect of the EFF suit is its emphasis on MediaMax. Most of the other lawsuits have focused on Sony's other copy protection technology, XCP. The EFF suit does talk about XCP, but only after getting through with MediaMax. Emphasizing MediaMax seems like a smart move — while Sony has issued an apology of sorts for XCP and has recalled XCP discs, the company is still stonewalling on MediaMax, even though MediaMax raises issues almost as serious as XCP.

As Alex wrote last week, MediaMax is spyware: it installs software without notice or consent; it phones home and sends back information without notice or consent; and it either doesn't offer an uninstaller or makes the uninstaller difficult to get and use. MediaMax lacks the rootkit-like feature of XCP, but otherwise MediaMax shares all of the problems of XCP, including serious security problems with the uninstaller (mitigated by the difficulty of getting the uninstaller; see above).

But even if all these problems are fixed, the MediaMax software will still erode security, for reasons stemming from the basic design of the software.

For example, MediaMax requires administrator privileges in order to listen to a CD. You read that right: if you want to listen to a MediaMax CD, you must be logged in with enough privileges to manipulate any part of the system. The best practice is to log in to an ordinary (non-administrator) account, except when you need to do system maintenance. But with MediaMax, you must log in to a privileged account or you can't listen to your CD. This is unnecessary and dangerous.

Some of the security risk of MediaMax comes from the fact that users are locked into the MediaMax music player application. The player app evades the measures designed to block access to the music; and of course the app can't play non-MediaMax discs, so the user will have to use multiple music players. Having this extra code on the system, and having to run it, increases security risk. (And don't tell me that music players don't have security bugs — we saw two serious security security bugs in Sony music software last week.) Worse yet, if a security problem crops up in the MediaMax player app, the user can't just switch to another player app. More code, plus less choice, equals more security risk.

Worse yet, one component of MediaMax, a system service called sbcphid, is loaded into memory and ready to run at all times, even when there is no disc in the CD drive and no music is being played. And it runs as a kernel process, meaning that it has access to all aspects of the system. This is another component that can only add to security risk; and again the user has no choice.

It's important to recognize that these problems are caused not by any flaws in SunnComm and Sony's execution of their copy protection plan, but from the nature of the plan itself. If you want to try to stop music copying on a PC, you're going to have to resort to these kinds of methods. You're going to have to force users to use extra software that they don't want. You're going to have to invoke administrator privileges more often. You're going to have to keep more software loaded and running. You're going to have to erode users' ability to monitor, control, and secure their systems. Once you set off down the road of copy protection, this is where you're going to end up.

This entry was posted on Tuesday November 22, 2005 at 3:51 am and is filed under Security, DRM, Privacy, CD Copy Protection. You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or trackback from your own site.

34 Responses to “More Suits Filed; MediaMax Insecurity Remains”

1. *Anonymous* Says:
   November 22nd, 2005 at 4:57 am

   “As Alex wrote last week, MediaMax is spyware…” Actually unless it was missed he fell short of actually calling it “spyware” by calling it “spyware like”.

   Still waiting for an evaluation of Macrovisions audio solution! While you have substantially evaluated 2 of the 3 solutions available Macrovision has somehow has escaped your scrutiny. In the fairness of reporting of course.

2. *windwalker* Says:
   November 22nd, 2005 at 4:59 am

   “As Alex wrote last week, MediaMax is spyware…” Actually unless it was missed he fell short of actually calling it “spyware” by calling it “spyware like”.

   Still waiting for an evaluation of Macrovisions audio solution! While you have substantially evaluated 2 of the 3 solutions available Macrovision has somehow has escaped your scrutiny. In the fairness of reporting of course.

3. *Anonymous* Says:
   November 22nd, 2005 at 5:28 am

   sorry about the double post, didn’t think the first one took without a name attached while it gave an error message.

4. *Bill Whitmore* Says:
   November 22nd, 2005 at 5:29 am

   Obviously another dumb SunnComm supporter who is reading impaired.

   “Actually unless it was missed he fell short of actually calling it “spyware” by calling it “spyware like”.”

   This is what Halderman wrote….

   Sony Shipping Spyware from SunnComm, Too
   ==============================

   http://www.freedom-to-tinker.com/?p=925

   Read it again…

   Sony Shipping Spyware from SunnComm, Too
   ==============================

   That doesn’t fall short of calling it Spyware. He called it Spyware. Once more, just for you…

   Sony Shipping Spyware from SunnComm, Too
   ==============================

   http://www.freedom-to-tinker.com/?p=925

Also, SunnComm dumbo. Here is an evaluation of CDS from Halderman.

http://www.cs.princeton.edu/~jhalderm/papers/drm2002.pdf

Its an earlier version, but he has evaluated CDS. Maybe when Macrovision sell a CDS-300 CD in the US, Alex might buy one and evaluate it. But until then, he is doing a great job protecting consumers from the likes of the trash put out by SunnComm.

5. *Steve* Says:
   November 22nd, 2005 at 6:21 am

   Very good analysis. I have long been tired of “partner” programs/links being installed on OEM versions of Windows and other software. I realize that companies hope that by being “visible” that we will be enticed to buy. But as everyone knows these unncessary programs “steal” resources, make our computer systems unreliable, and are difficult to remove. One can only hope that the rootkit scandle has awakend a sense of ethics in the corporate world not to tresspass on our computers. Fingers crossed.

6. *TomCS* Says:
   November 22nd, 2005 at 7:58 am

   Are there any significant differences between Mediamax/Win and Mediamax/OS X? The analysis,for which I am very grateful, seems primarily Windows/autorun focussed.

7. *Paul* Says:
   November 22nd, 2005 at 11:18 am

   I’m not clear on one point. You said:

   “…including serious security problems with the uninstaller (mitigated by the difficulty of getting the uninstaller; see above).”

   Did you mean “exacerbated by” instead of “mitigated by”? It seems that the difficulty of obtaining an uninstaller for this software would make the security problem worse (exacerbate it), not make it less of an issue (mitigate it). Am I reading this wrong?

8. *Anonymous* Says:
   November 22nd, 2005 at 11:31 am

   “Did you mean “exacerbated by” instead of “mitigated by”? It seems that the difficulty of obtaining an uninstaller for this software would make the security problem worse (exacerbate it), not make it less of an issue (mitigate it). Am I reading this wrong?”

   Mitigate would be correct in this case!

   ” Shortly after becoming aware of the problem, SunnComm had patched the downloadable software. After completing the patch, testing was conducted by Professor Felten’s team at Princeton. Immediately upon notification of successful testing, the updated program was made available to those CD buyers who requested it. This security issue existed on the downloadable MediaMax uninstaller and removal program only – not on the CDs themselves.”

9. *Tommy Knowlton* Says:
   November 22nd, 2005 at 11:32 am

   > One can only hope that the rootkit scandle has awakend a sense of ethics in the corporate world not to tresspass on our computers. Fingers crossed.

   More likely, the lesson will be to work harder to avoid being caught. Remember that the driving force behind including this software in the first place was revenue protection. Nothing’s changed in that regard. The content industry still considers its customers' behavior to be a threat, and they still want to control the product after the sale.

10. *Riley* Says:
November 22nd, 2005 at 12:43 pm

Isn't that the rub though? The harder these companies try to hide their actions, the more sinister they look when they are uncovered. Not to mention, you simply are NOT going to hide forever no matter how successful you are and as your reputation worsens, so does the number of people working to uncover your secrets. Every SonyBMG CD for the next few years will be scrutinized beyond belief with everyone trying to become the next 'Mark' to out Sony and make a name for themself. Not to mention - if the security companies are smart, they will also be scrutinizing these things as well so they don't have a repeat situation where they look like idiots that are unable to stop a direct attack to rootkit your computer.

Something that may have changed for these companies is if their execs come to the conclusion that their anti-piracy measures are actually costing the company more money than they are saving them. Sony's financial statements for the next few quarters will be telling - how much will this cost them and how will the lawsuits pan out? Money talks - and it may be talking loud enough after this fiasco for the execs to hear it.

11. *tobias robison* Says:
November 22nd, 2005 at 3:51 pm

Is it possible that 500,000 networks are infected because many other non-SONY CDs are out there with the same DRM on them? Is anyone trying to determine what other CD manufacturers are playing this game?

12. *mrszilch* Says:
November 22nd, 2005 at 4:00 pm

I have 2 CDs with MediaMax. I contacted SunnComm for removal of their spyware. The following is their response. They don't seem to care about the problems their softeare & then initial uninstall process causes. I have not been able to play any original music CD since MediaMax was installed on my computer. I especially appreciate their "Have a Fine Day!" comment.

"Your ticket 031131 has been Answered

We apologize if this disc did not meet your needs. It is ever our endeavor to meet the needs of all consumers by providing a visually enhanced multimedia environment while still protecting the rights of your favorite artist. As requested, we have included a link below that will take you to a brand new uninstall utility that will remove all files related to the MediaMax application.

Please note a few things:

First of all, if you are running Windows XP with service pack 2, you may not receive the request to install ActiveX control to perform the uninstall due to the default security settings associated with the service pack. When you are presented with a blank window, please click on the line at the top of the page which will give you the option to install ActiveX control and then proceed removal. (note: the ActiveX control installed will be removed upon your next reboot)

Secondly, before completion of the removal, you will receive a window which lists common system files that were shared by the MediaMax application. These files will not be affected by this uninstall because they are files not associated directly with MediaMax, and may be necessary for the functions of other software installed on your PC.

Please click here and follow instructions to remove MediaMax:

http://www.sunncomm.com/support/tools/removal.asp

Thank you very much and we do hope you have a fine day!

SunnComm Technical Support Team”

13. *Richard* Says:
November 22nd, 2005 at 8:54 pm

The removal tool is now posted from Sunncomm’s help page (URL is on the back of every MediaMax-infected CD). The removal tool is the same link as in the previous message. I see it’s another ActiveX program, but no personal information. But did they fix the security issues?

14. *Anonymous* Says:
November 22nd, 2005 at 11:10 pm

The post below, by Peter Jacobs, CEO of SunnComm was made after Halderman’s first report on MediaMax. Isn’t it ironic that Sony has now forced SunnComm to go cap in hand to Halderman to seek his endorsement that the new Uninstaller is written correctly.

msg# 1480 Date:10/13/2003 2:01:49 AM
Post #of 1552

Steve and gang,

My biggest problem with the Halderman Report was that he has an undisclosed agenda and he is insincere.

The agenda (you already know) is the EFF, and, when you think of it, there is an exact parallel between the JDF and EFF.

It’s insincere because they whined about other protection technology causing playability problems (which is understandable, kinda), but to criticize MediaMax for not being secure enough is laughable, considering the position of the EFF which is that no stuff ought to be secured, and people should be left to their own conscience (or, if they’re caught, then prosecuted) when it comes to digital property theft.

I’ll bet none of them EVER had any digital content that anyone else (aside from family and friends) would pay for, and, if they did, they’d be screaming bloody murder if someone ripped them off.

Halderman then publishes a how-to on getting our License Mgt Technology out of the PC by naming the hidden file (which the user has given us permission to put there)…clearly in violation of the DMCA, all while making the press believe we’re pissed because he “found” the shift key workaround.

Last, he misrepresented his so-called “shift key” discovery (which had been reviewed by Piper Jaffray and others over a month ago, made it seem like HE discovered it, and made us look like idiots and charletons so he could achieve his 15 minutes of fame. He also implied that the record companies were not in possession of full knowledge about the workings of MediaMax (after almost a year of trials).

5,000 emails later…the vilest crap you’d every want to get from “information freedom fighters” at the EFF…I’m looking foward to a productive and more normal week.

Hope you all do to. Let’s take it back.

pj

http://www.ragingbull.lycos.com/mboard/boards.cgi?board=STEH&read=52960

15. *Anonymous* Says:
November 22nd, 2005 at 11:19 pm

Another slur on Halderman from Peter Jacobs, CEO of SunnComm

Q: What makes you think that the DCMA gives you the right to violate someone´s first amendment rights, and sue them for talking about a commonly known feature of the Windows operating system? Besides that, do you not think that this oppression of speech could lead to even worse violations of our rights?

(10/27/2003 10:44:13 AM)

A: My friend, I´m going to print your letter as it represents the 1000´s of emails I´ve received from like-minded people who, like you, didn´t bother to read enough to understand the Princeton situation.

SunnComm´s position was that Mr. Halderman violated the DMCA by revealing the hidden MediaMax management file name that is placed on a user´s PC, along with instructions on how to remove it.

The SunnComm-alleged violation had NOTHING to do with the Shift Key. He knows it and we know it.

By publicly saying things like, “Gee, if telling people about the Shift Key is a violation of the DMCA, then we need to change that bad law,” Halderman is purposely mis-directing the debate, and, by doing so, stoops to a level far below that of his adversaries. The ends NEVER justify the means. I think he´s had enough computer science classes. He needs some time in morality class.

Sorry for the long response, but you did ask me what I thought.

Sincerely,

Peter

http://ragingbull.lycos.com/mboard/boards.cgi?board=STEH&read=59514

16. *PaulT* Says:
November 23rd, 2005 at 4:04 am

The fun thing is read the uninstall instructions on the sunncomm website -

Quote: “Is there a way to remove your software from my computer?”

Response “Please note that MediaMax was designed to manage and safeguard the copyrights of specified artists’ CDs while giving you an enhanced visual and listening experience. It does not interfere with or impact any of the normal operations and/or functions of your computer.
”
- http://tickets.sunncomm.com/selfhelp/addbook_readarticle.php?articleID=24

17. *Code Monkey* Says:
November 23rd, 2005 at 7:02 am

I think it was a very shrewd move by Sunncomm to bring Alex H. and Ed F. into their team. This new CEO they brought over from BMG knows their stuff and should be able to solidly lock SonyBMG into the MediaMax system. Industry standard isn’t far off now. Looks like Alex and Ed are now part of the winning development team.

18. *Ed Felten* Says:
November 23rd, 2005 at 7:14 am

CodeMonkey,

Alex and I have not joined SunnComm’s team.

Our longstanding policy is that when we find a serious security flaw in a company’s product, as we did with SunnComm’s, we offer to discuss that flaw with the vendor and to test any proposed patch they have. We do this to help protect customers who have been put at risk by the vendor’s security errors.

When we do this, it is not an endorsement of a vendor or its products. Indeed, it only becomes necessary when the vendor has put its customers at risk.

19. *mrszilch* Says:
    November 23rd, 2005 at 7:32 am

    Ed,
    Is this new patch from SunnComm OK to use? I want MediaMax off my computer but not at the risk of opening security hole. Thanks

20. *Anonymous* Says:
    November 23rd, 2005 at 7:45 am

    Ed Felten Says: [I’m not sure what he is trying to quote here, but don’t be fooled into thinking that any of the stuff below came from me. — Ed Felten]

    It has the appearance of being disingenuous by not posting the patch here and report that MediaMax has provided such a patch immediately after your testing and analysis.

    Will we soon be seeing your analysis of Macrovisions DVD Ripguard technology which has hit the market and has been immediately ripped?

21. *Anonymous* Says:
    November 23rd, 2005 at 7:59 am

    Ed has already given an appraisel of Ripguard. Don’t SunnComm people check anything.

    It was a negative appraisel, which shoots down SunnComm’s claims that Freedom-To-Tinker’s uncomplimentary analyses of MediaMax is because they are doing it on behalf of Macrovision.

    http://www.freedom-to-tinker.com/?p=768

22. *Anonymous* Says:
    November 23rd, 2005 at 8:10 am

    Given that analysis by Porf Felton it seems there is not an uninstall to get ripguard off of my puter, and unlike the new MediaMax uninstall analysed by the Priceton boys, I worry that there may be some hazard caused to my computer.

    Does Ripguard have security risks for my puter?

23. *Code Monkey* Says:
    November 23rd, 2005 at 8:25 am

    Ed Felten, I guess I misinterpreted the news I read. Sorry {{:^(

    Does your latest testing show that MediaMax is a safe and viable DRM tool now?

24. *Ed Felten* Says:
    November 23rd, 2005 at 8:25 am

    People are claiming that SunnComm has released a new uninstaller, but (1) they haven’t told me that have released one, (2) I haven’t seen it in the press, and (3) I can’t find the new uninstaller on SunnComm’s web site.

25. *Ed Felten* Says:

November 23rd, 2005 at 8:29 am

Somebody pointed me to the new MediaMax uninstaller. We haven’t yet verified that it is the same code we tested. Assuming it is the same, then it does not suffer from the serious security flaw that the previous uninstaller had.

26. *Anonymous* Says:
November 23rd, 2005 at 8:40 am

“Given that analysis by Porf Felton it seems there is not an uninstall to get ripguard off of my puter, and unlike the new MediaMax uninstall analysed by the Priceton boys, I worry that there may be some hazard caused to my computer.”

If you understood Prof Felton’s analysis, you would have realized that Ripguard doesn’t install anything on the computer. It provides passive protection.

27. *Ed Felten* Says:
November 23rd, 2005 at 8:56 am

Code Monkey,

See the blog entry on which you were commenting for more on this. Here’s a brief quote: “But even if all these problems are fixed, the MediaMax software will still erode security, for reasons stemming from the basic design of the software.”

28. *Anonymous* Says:
November 23rd, 2005 at 11:33 am

Prof Felton:
How can you possibly post that you haven’t tested Sunncomms patched uninstaller this morning when sunncomm on Nov 19 stated your team had tested it?

Somebody pointed me to the new MediaMax uninstaller. We haven’t yet verified that it is the same code we tested. Assuming it is the same, then it does not suffer from the serious security flaw that the previous uninstaller had.

MediaMax Technology Statement Regarding Potential Security Issue
MediaMax released this statement regarding the potential security issue associated with the MediaMax uninstaller program

November 19, 2005 – MediaMax Technology Corp. (OTCBB:MMXT), stated today that SunnComm International (OTC:SCMI), the maker of MediaMax has patched a potential security issue identified by J. Alex Halderman from Princeton University.

The incoming president and CEO of MediaMax Technology, Kevin M. Clement explains, “the SunnComm and MediaMax teams responded immediately upon notification of a potential security issue associated with an uninstaller tool used to remove MediaMax from users’ computers Notification has been sent to 223 individuals who have requested a removal tool over the past two plus years. All of those users have been notified of the situation and provided instructions for removing the affected software along with any potential security risk.”

“We sincerely apologize for any inconvenience this may have caused. We also want to thank Professor Edward W. Felten, J. Alex Halderman and the Princeton team of computer experts.”

Shortly after becoming aware of the problem, SunnComm had patched the downloadable software. After completing the patch, testing was conducted by Professor Felten’s team at Princeton. Immediately upon notification of successful testing, the updated program was made available to those CD buyers who requested it. This security issue existed on the downloadable MediaMax uninstaller and removal program only – not on the CDs themselves.

29. *Anonymous* Says:

November 23rd, 2005 at 8:00 pm

This is not about genuine technology, it is about the distaste for protecting the “ability for consumers right to copy” plain and simple, regardless of the artist and the artist work!

Just a cloak for tearing down some ones work, plain and simple.

“But even if all these problems are fixed, the MediaMax software will still erode security, for reasons stemming from the basic design of the software.”
And just how is that? Please explain! Or is it “characteristic of” or “spyware like”? Can you pin it down a bit better?

You Mr Felton and your class clowns are pathetic and very lacking in your genuine altruistic endeavors in the name of science. LOL

Get used to it!

30. *Anthony Youngman* Says:
November 25th, 2005 at 6:56 am

Humm….

I like the SunnComm guy’s comments about how “the user gave permission to install the software”. What about all the reports that say “even after clicking NO to the agreement box, it went ahead and installed anyway”.

And while I have no proof it was MediaMax, seeing as it was on a Sony-BMG CD I suspect it was, my system got trashed when I tried to play a Rod Stewart CD. And I definitely did not give it permission to do anything, because at NO POINT WHATSOEVER did it ask for permission …

Cheers,
Wol

31. *Edward Kuns* Says:
November 25th, 2005 at 4:12 pm

Really? “The user gave permission to install the software”? Not me, yet the software was installed on my employer’s computer when I just wanted to listen to a music CD. I rejected the ridiculous EULA and didn’t want to be stuck with one music player for that CD instead of the music player I choose to use for all of my other music. Yet, there was already a driver installed onto my employer’s computer.

The trolls here are getting annoying, and they stand out obviously as trolls. I can’t imagine that they believe they will sway anyone’s opinion with their nonsensical logic and inability to take the full context of something into account before responding. The duplicity in the trolls’ posts is astonishing in its depth.

32. *Jesse Weinstein* Says:
December 12th, 2005 at 2:10 am

Testing. The last comment resulted in the error message: “This comment has been logged, and will not be displayed on the blog.”

33. *Jesse Weinstein* Says:
December 12th, 2005 at 2:10 am

Testing. The last comment resulted in the error message: “This comment has been logged, and will not be displayed on the blog.” …

34. *EFF: SunnComm MediaMax Security Vulnerability FAQ* Says:
January 10th, 2006 at 9:34 pm

[…] What is the SunnComm MediaMax Security Vulnerability? Certain audio compact discs distributed by Sony BMG contain a version of the SunnComm MediaMax software, which creates a serious risk of a “privilege escalation attack.” This new security vulnerability — different than the one reported in early November regarding Sony BMG CDs sold with software called XCP — affects all Sony BMG CDs that contain version 5 of SunnComm MediaMax software. According to Sony BMG, about six million CDs have this software. Sony BMG’s list of affected CDs Is there a solution? On Tuesday December 6, Sony BMG and SunnComm made available a patch that was designed to resolve this security vulnerability. We’re pleased that Sony BMG responded quickly and responsibly when we drew their attention to this serious security problem. However, the day after the patch was released, Professor Ed Felten and Alex Halderman identified a new problem. Sony BMG has now released a second patch, which security researchers are reviewing. What is a privilege escalation attack? A privilege escalation attack is the act of exploiting a security weakness in an application to gain access to resources that normally would have been protected from an application or user. This means that low-rights users can add files to a directory and overwrite the binaries installed therein, which will be then be unknowingly executed by a later user with higher level of rights. In other words, a guest user or a malicious program can effectively make changes to a computer that would normally be reserved to an administrator. Can you explain this with an analogy? Consider an office worker who has keys to her office and to the front door of the building, but not to other offices or to the supply closet. There are many ways to gain additional access: Sometimes those locks can be picked, sometimes the locks are left unlocked, and sometimes an attacker can steal the building manager’s keys. This vulnerability is yet another way to gain increased access, similar to leaving the manager’s keys out. By stealing the manager’s keys, the office worker can escalate her privileges, i.e. get into offices and other room where she is not authorized. What are access controls? On a computer system, information resources are protected with access controls analogous to door locks. A common implementation of such access controls is called an access control list (ACL). An ACL is simply a table listing principals (e.g. user accounts) and the privileges each principal has with an object. An ACL might stipulate, for example, that user account Bob can read the spreadsheet file accounts-2005.xls, while user account Jane can both read and write it. In this example, the Bob and Jane accounts are principals, the accounts-2005.xls file is the object, and “read” and “write” are privileges. What are some details of the MediaMax vulnerability? MediaMax version 5 leaves a crucial folder “unlocked,” that is to say with an ACL that allows all principals to have all privileges. The reason this is a problem is that the folder contains an executable program (MMX.EXE, the MediaMax program) that must be run by a user account with high privileges. An attacker can overwrite MMX.EXE with code of her choice, and the next time a MediaMax disc is played, her attack code will be executed. Specifically, the directory that the SunnComm MediaMax software creates, located in “c:Program FilesCommon FilesSunnComm Shared,” overrides the default Access Control List (also known as the file system permissions). The SunnComm Shared directory uses an ACL that doesn’t protect against low rights users (i.e., “Everyone” in Windows parlance) overwriting the contents including the installed binaries. Returning to our example of Bob and Jane, it mean that Bob can now rewrite the spreadsheet, or more worrisome, replace it with a malicious program. How could this harm consumers’ computer? The SunnComm MediaMax version 5 software distributed by Sony BMG could expose the computers of millions of users to attacks by malicious hacker and virus writers. They undermine significant security protections otherwise present on computers running Windows, which are designed to prevent users (either people or programs) from gaining control of your computer. Who discovered the MediaMax security vulnerability? iSEC Partners discovered the security vulnerability after EFF requested an examination of the software, and EFF and iSEC promptly communicated it to Sony BMG. In accordance with standard information security practices, EFF and iSEC delayed public disclosure of the details of the exploit to give Sony BMG the opportunity to develop a patch. iSEC Partners’ report [PDF, 237K] Who is iSEC Partners? iSEC Partners is a proven full-service security consulting firm that provides penetration testing, secure systems development, security education and software design verification. iSEC Partners’ security assessments leverage their extensive knowledge of current security vulnerabilities, penetration techniques and software development best practices to enable their customers to secure their applications against ever-present threats on the Internet. Primary emphasis is placed upon helping software developers build safe, reliable code. Areas of research interest include application attack and defense, web services, operating system security, privacy, storage network security and malicious application analysis. For more information: http://www.isecpartners.com. Are there any more security issues with SunnComm’s MediaMax software? We don’t know. We have identified one security issue, but there may be others. Even before this vulnerability came to light, security researcher Ed Felten noted “the MediaMax software will still erode security, for reasons stemming from the basic design of the software.” See Freedom to Tinker for more. We urge Sony BMG to undertake rigorous security testing on all of its software, and we will continue to look into this issue. How many CDs are affected? There are over 20 million Sony BMG CDs with some version of the SunnComm MediaMax software. Sony BMG says that about six million have the MediaMax version 5 that is subject to this vulnerability, and has provided a list of affected titles. In addition EFF has prepared a Spotter’s Guide to help you identify MediaMax CDs in the wild. Sony BMG’s list of affected CDs EFF’s Spotter’s Guide What are some of the artists with SunnComm MediaMax CDs? MediaMax can be found on a wide variety of popular artists’ music, such as Britney Spears “Hitme (Remix)” , David Gray’s “Life In Slow Motion,” My Morning Jacket’s “Z,” Santana’s “All That I Am,” and Sarah McLachlan’s “Bloom (Remix Album).” Sony BMG’s list of affected CDs EFF’s list of CDs affected and possibly affected by MediaMax. Does the patch resolve all the issues with CDs with SunnComm MediaMax software? No.

> There are other severe problems with MediaMax discs, including: undisclosed communications with servers Sony controls whenever a consumer plays a MediaMax CD; undisclosed installation of over 18 MB of software regardless of whether the user agrees to the End User License Agreement; and failure to include an uninstaller with the CD. EFF will continue to raise these issues with Sony BMG. Does SunnComm MediaMax appear on CDs other than those released by Sony BMG? Yes. According to SunnComm, its "MediaMax technology has appeared on over 140 commercially released CD titles across more than 30 record labels." Earlier this year, SunnComm forecast "that its MediaMax CD Copy Management Technology will be Applied to More than 145,000,000 Audio CDs this Year." Currently our focus is on the Sony BMG CDs, but we are investigating whether the vulnerability exists on other labels, and urge every label that has used the MediaMax technology to check with security experts immediately. SunnComm press release: SunnComm Ups Security Another Notch SunnComm press release: SunnComm Forecasts for MediaMax Is EFF Suing Sony BMG? Yes. On November 21, EFF, along with the law firms of Green Welling, LLP, and Lerach, Coughlin, Stoia, Geller, Rudman and Robbins, LLP, filed a California class action lawsuit in Los Angeles against Sony BMG including claims arising from both XCP and SunnComm CDs. We also filed a national class action on December 2 in New York and are joined in that action by the Law Offices of Lawrence E. Feldman and Associates. Sony BMG litigation information What more does EFF want Sony BMG to do? EFF would like Sony BMG and all record labels to stop using DRM on their CDs and stop requiring its customers to agree to a EULA as a condition of playing CDs on their computers. See: The Customer is Always Wrong, DRM Skeptics View, and New York Times Op-Ed: Buy, Play, Trade, Repeat. Barring that, we would like Sony BMG to ensure, before a CD is released to the public, that it contains no security vulnerabilities, can be fully uninstalled by end users, properly protects consumer privacy including allowing consumers to opt-out of any reporting back to the company done by the CD, and is provided on terms that are fair, reasonable and fully disclosed. To the extent that they fail to do so, they need to remove such products from the market immediately, engage in a robust notice campaign and compensate consumers who have purchased them, including those harmed by XCP and MediaMax software already. […]

Leave a Reply

Name

Mail (will not be published)

Website

Submit Comment

Powered by WordPress.
Entries (RSS) | Comments (RSS).